

ATTENTION

The following documents appearing in FBI files have been reviewed under the provisions of The Freedom of Information Act (FOIA) (Title 5, United States Code, Section 552), Privacy Act of 1974 (PA) (Title 5, United States Code, Section 552a), and/or Litigation

☐ FOIA/PA

☐ Litigation

☐ Executive Order Applied

Requester _____
 Subject _____
 Computer or Case Identification Number _____
 Title of Case _____ Section _____
 * File _____
 Serials Reviewed _____

 Release Location *File _____ Section _____

This file section has been scanned into the FOIPA Document Processing System (FDPS) prior to National Security Classification review. Please see the documents located in the FDPS () for classification action, if warranted. Direct inquiries about the FDPS to RIDS Service Request Unit, 202-321- b2

File Number 288A-SF-133411-1A Section 1
 Serial(s) Reviewed ALL

FOIPA Requester _____
 FOIPA Subject _____
 FOIPA Computer Number 991994

File Number _____ Section _____
 Serial(s) Reviewed _____

FOIPA Requester _____
 FOIPA Subject _____
 FOIPA Computer Number _____

File Number _____ Section _____
 Serial(s) Reviewed _____

FOIPA Requester _____
 FOIPA Subject _____
 FOIPA Computer Number _____

THIS FORM IS TO BE MAINTAINED AS THE TOP SERIAL OF THE FILE, BUT NOT SERIALIZED

ATTENTION

DO NOT REMOVE FROM FILE

~~SF 133411~~

1A's

133411

Vol 5,

(1-)

~~133411~~
1
3
3
3
4
1
1

~~288A~~

288A

C 7/2/03

~~London~~

1A Envelope

Case ID: 288A-SF-133411-1A

SF	1	!	ORIGINAL NOTES RE INTERVIEW OF	[REDACTED]	!			
SF	2	!	WEBSITE	[REDACTED]	!			
SF	3	!	WHO IS ON	[REDACTED]	!			
SF	4	!	ORIGINAL NOTES RE INTERVIEW OF	[REDACTED]	ON 1/16/2003	!		
SF	5	!	WHO IS	[REDACTED]	!			
SF	6	!	EMAIL ON 1/8/03		!			
SF	7	!	EMAIL 1/16/2003		!			
SF	8	!	[REDACTED] WEB PAGES ON DISK AND PAPER		!			
SF	9	!	WHO IS ON	[REDACTED]	!			
SF	10	!	FLOPPY DISK CONTAINING EMAIL AND ATTACHMENTS (1-6-2003)		!			
		!	(13:30:00)		!			
SF	11	!	ORIGINAL NOTES RE INTERVIEW OF	[REDACTED]	!			
SF	12	!	CD'S OF	[REDACTED]	MACHINE FROM	[REDACTED]	b7C	!
SF	13	!	[REDACTED] IP SCAN			b7D	!	
SF	14	!	[REDACTED] IP SCAN			b2	!	
SF	15	!	[REDACTED] IP SCAN			b3	!	
SF	16	!	SOURCE EMAILS				!	
SF	17	!	EMAIL FROM	[REDACTED]	WITH BOT ATTACHMENTS		!	
SF	18	!	ONE CD ROM CONTAINING IRC LOG	[REDACTED]			!	
SF	19	!	EMAIL				!	
SF	20	!	ONW (1) CDR WITH IRC LOG OF	[REDACTED]	CHANNEL	[REDACTED]	!	
SF	21	!	[REDACTED] SUBPOENA RETURN				!	
SF	22	!	PHOTO ON 3.5" FLOPPY OF	[REDACTED]			!	
		!	NOTES FROM	[REDACTED]	PHONE CALL		!	
		!	FAX OF ITEM SEIZED				!	
		!	NOTES FROM	[REDACTED]	ON	[REDACTED]	!	
		!	[REDACTED] APP AND AFF				!	
SF	23	!	ORIGINAL NOTES RE INTERVIEW OF	[REDACTED]			!	
SF	24	!	ORIGINAL NOTES RE INTERVIEW OF	[REDACTED]			!	
		!					!	
		!					!	

1A (1)

Universal Case File Number 288A-SF-133411Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document _____

Date Received 1-3-2003 b7CFrom [REDACTED] b7D

(Name of Contributor)

(Address of Contributor)

(City and State)

b7C

By SA [REDACTED]To Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ NoTitle: UNSUB(S);
GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - ImpairmentReference: FD-302 DATED 1-3-2003

(Communication Enclosing Material)

Description: ☒ Original notes re interview of b7C

b7D

288A-SF-133411 1A (1)

1-3-03

① 9:23a

[redacted] - Proc

(e) [redacted] b7C

Google Security b7D

(e) [redacted]

(e)

(e)

Google

General Counsel

[redacted]

[redacted]

[redacted]

b3

- Attacks

② 10:00a

1-2 am (PST 8a)

b7C

[redacted] [redacted] [redacted]

b7D

[redacted]

Detected attack on Google

per 4a PST on 1-2-03 attack

Google checked logs noticed

5-7 min (UDP flood, ping flood)

[redacted] included > 4,000 hosts dist DoS
network handled traffic, close to fail

later afternoon, before 3p PST

hit again, syn flood

large scale, global effect on network

1 out of 3 incoming searches affected

5-7 min

b7C

[redacted] said IAC server hostine [redacted] failed

b7D

[redacted] failed reconnecting [redacted] missed

(the time attack hit

assume it's the same person (Google)

[redacted] - global threat - name from log entry
commands issued to [redacted]

b7C

[redacted]

gt - global threat - at one point affiliated
with [redacted]

b7C

b7C

b7D

gave [redacted] info
to local FBI

Servers attacked - Santa Clara, Virginia

1. - Santa Clara only
2. - both

Google checking logs for IP's/spoofing

Most of bots live on [redacted] (class "A")

b7C

b7D

[redacted] uses channels of [redacted]
makes [redacted] a target

b2

Damages - working numbers (def > \$5,000)

1A(2)

Universal Case File Number 288A-SF-133411Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document _____

Date Received 1-16-2003

From _____

(Name of Contributor)

(Address of Contributor)

(City and State)

By SA

b7C

To Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ NoGrand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ NoTitle: UNSUB(S);
GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment
01/02/2003Reference: FD-302 1/15/03

(Communication Enclosing Material)

SERIAL 6Description: ☐ Original notes re interview ofWEBSITE

b7C

288A-SF-133411-1A(2)



1-16-2003

WEBPAGES

b7C

b7C

Show me how to:



[Home](#) [Your Account](#) [Downloads](#) [Submit News](#) [Topics](#)

b7C

Unregistered.

b7C

You are an unregistered user, Please register, its FREE! thanks. registering offers many enhancements, including customizable themes, headlines, webmail etc. So check it out!

- [Home](#)
- [AvantGo](#)
- [Chat](#)
- [Downloads](#)
- [Feedback](#)
- [Journal](#)
- [Private Messages](#)
- [Recommend Us](#)
- [Search](#)
- [Statistics](#)
- [Stories Archive](#)
- [Submit News](#)
- [Surveys](#)
- [Top 10](#)
- [Topics](#)
- [Web Links](#)
- [WebMail](#)
- [Your Account](#)

IRCd Up!

IRCd up! use (if it doesnt resolve, use Thanks!

Update!

b7C

Own a shell/webhosting provider now! Cheap, High Quality shell's, Hosting: bots, websites, IRCd's, and more! We will also custom-build shells for you for any type of hosting you can think of! is the solution for your hosting needs!

Community

[Forums](#)

b7C

Languages

Select Interface Language:

User:

b7C

Welcome, **Anonymous**

Nickname

Password

(Register)

http:

b7C

1/16/2003



b7C



Membership:



Latest 



New Today: **0**



New Yesterday: **0**



Overall: **16**



People Online:



Visitors: **3**



Members: **0**

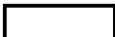



Total: **3**

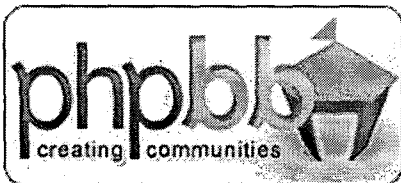
Hits

We received
3255
page views since
November 18, 02

b7C

Copyright© 2002 by 
Site owned and maintained by 

b3



The IRC Bot related forum

b7C

[FAQ](#) [Search](#) [Memberlist](#) [Usergroups](#) [Register](#)
[Profile](#) [Login to check your private messages](#) [Login](#)

The time now is Wed Jan 15, 2003 5:22 pm

Forum Index

[View unanswered posts](#)

Forum	Topics	Posts	Last Post
Bots			
General Bot Talk Talk generally about IRC bot's, zombies, drones. this is NOT a trading channel, to trade visit the bot trading section. Thanks.	1	1	Wed Nov 20, 2002 2:53 pm
forum Forum dedicated to to get your own forum on for your own bot, drop a privmsg to and it will be promptly added.	2	3	Wed Dec 04, 2002 5:27 am

b7C

Mark all forums read

All times are GMT

Who is Online

Our users have posted a total of **4** articles
We have **4** registered users



The newest registered user is

b7C

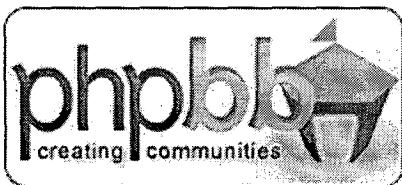
In total there is **1** user online :: 0 Registered, 0 Hidden and 1 Guest [Administrator] [Moderator]
Most users ever online was **2** on Tue Nov 19, 2002 1:37 am
Registered Users: None

This data is based on users active over the past five minutes

LoginUsername: Password: Log me on automatically each visit ☐

New posts No new posts Forum is locked

Powered by phpBB 2.0.3 © 2001, 2002 phpBB Group



The IRC Bot related forum

- [FAQ](#)
[Search](#)
[Memberlist](#)
[Usergroups](#)
[Register](#)
[Profile](#)
[Login to check your private messages](#)
[Login](#)

b7C

Forum Index

Select sort method: **Joined Date** Order **Ascending** **Sort**

#		Username	Email	Location	Joined	Posts	Website
1					19 Nov 2002	1	
2					20 Nov 2002	1	
3					26 Nov 2002	0	
4					01 Dec 2002	0	

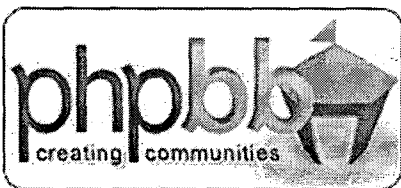
Page 1 of 1

All times are GMT

Jump to: **Select a forum** **Go**

Powered by phpBB 2.0.3 © 2001, 2002 phpBB Group

b7C



[]
The IRC Bot related forum

b7C

[FAQ](#) [Search](#) [Memberlist](#) [Usergroups](#) [Register](#)
[Profile](#) [Login to check your private messages](#) [Login](#)

when i come here like 10 das ago...

[newtopic](#) [postreply](#) [] Forum Index -> [] forum

[View previous topic](#) :: [View next topic](#)

Author

Message

[]
Guest

Posted: Thu Nov 28, 2002 11:35 am Post subject: when i come here like 10 das ago...

[quote](#)

when i come here 10 days ago...i see the **info** of new version of [] .and i see something like psybnc....feature....**is** this real? and..**is** posible to **implement in** next versions ? thanks..

b7C

[Back to top](#)

[]
Guest

Posted: Tue Dec 03, 2002 6:22 am Post subject: anybody here have the [] manual

[quote](#)

anybody here have the [] manual

[Back to top](#)

Display posts from previous: [All Posts](#) [Oldest First](#) [Go](#)

[newtopic](#) [postreply](#) [] Forum Index -> [] forum

All times are GMT

b7C

Page 1 of 1

Jump to: [] forum [Go](#)

You **can** post new topics in this forum
You **can** reply to topics in this forum
You **cannot** edit your posts in this forum
You **cannot** delete your posts in this forum
You **cannot** vote in polls in this forum

Powered by phpBB 2.0.3 © 2001, 2002 phpBB Group

b7C



[redacted]
The IRC Bot related forum

[FAQ](#) [Search](#) [Memberlist](#) [Usergroups](#) [Register](#)
[Profile](#) [Login to check your private messages](#) [Login](#)

b7C

where is it???

[newtopic](#) [postreply](#) [Forum Index](#) -> [forum](#)

[View previous topic](#) :: [View next topic](#)

Author

Message

[redacted]
Guest

[Posted](#): Wed Dec 04, 2002 5:27 am Post subject: where is it???

[quote](#)

[redacted] when r u gonna have [redacted] up for download? if u cant find a place to host it just host it @ [redacted] ask [redacted] for pass until u can find a better place

b7C

[Back to top](#)

Display posts from previous: [All Posts](#) [Oldest First](#) [Go](#)

[newtopic](#) [postreply](#) [Forum Index](#) -> [forum](#)

All times are GMT

Page 1 of 1

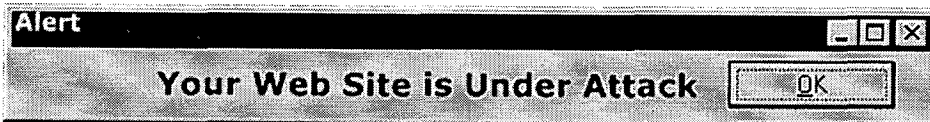
Jump to: [forum](#) [Go](#)

b7C

You **can** post new topics in this forum
You **can** reply to topics in this forum
You **cannot** edit your posts in this forum
You **cannot** delete your posts in this forum
You **cannot** vote in polls in this forum

Powered by phpBB 2.0.3 © 2001, 2002 phpBB Group

b7C



- [Home](#)
- [AvantGo](#)
- [Chat](#)
- [Downloads](#)
- [Feedback](#)
- [Journal](#)
- [Private Messages](#)
- [Recommend Us](#)
- [Search](#)
- [Statistics](#)
- [Stories Archive](#)
- [Submit News](#)
- [Surveys](#)
- [Top 10](#)
- [Topics](#)
- [Web Links](#)
- [WebMail](#)
- [Your Account](#)

Community

[Forums](#)

Languages

Select Interface
Language:

English

Users:

Welcome,
Anonymous

Nickname

Password

(Register)

- Unregistered.

You are an unregistered user, Please register, its FREE! thanks. registering offers many enhancements, including customizable themes, headlines, webmail etc. So check it out!

IRCd Up!

IRCd up! use (if it doesnt resolve, use Thanks!

Update!

owners of Own a shell/webhosting provider now! Cheap, High Quality shell's, Hosting: bots, websites, IRCd's, and more! We will also custom-build shells for you for any type of hosting you can think of is the solution for your hosting needs!

b7C

b7C

http://

b7C

1/15/2003

1A(3)

Universal Case File Number 288A-SF-133411Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document _____

Date Received 1-16-2003

From _____

(Name of Contributor)

(Address of Contributor)

(City and State)

By SA

b7C

To Be Returned ☐ Yes ☐ NoReceipt Given ☐ Yes ☐ NoGrand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure☐ Yes ☐ No

Federal Taxpayer Information (FTI)

☐ Yes ☐ NoTitle: UNSUBS;
GOOGLE.COM - VICTIMReference: FD-302 DATED 1/16/03

(Communication Enclosing Material)

SERIAL 7Description: ☐ Original notes re interview ofWHOIS ON

b7C

288A-SF-133411-1A(3)

[home](#) | [register a new domain](#) | [my DotTK](#) | [about DotTK](#) | [support](#) | [policies](#) | **WHOIS**

WHOIS

WHOIS

Selected domain name

This is a PAIDDOMAIN.TK domain name. On this domain name the PAIDDOMAIN.TK terms and conditions apply.

The registrant of this domain name is:

Company

Name

Address

Postal code/zipcode

City

State

Country

Phone number

Fax number

Email address

Name servers

b7C

WHOIS search on another domain name

WWW. .TK

CONTINUE >>

REGISTER A DOMAIN

Find your domain name now!

.tk

OK >>

> Want to know why it's free?

DOT TK SERVICES

Dot TK Domain names

- > [How does it work?](#)
- > [Increasing your traffic](#)
- > [Become a Dot TK Affiliate](#)
- > [Fortune 500 Trademark Trade](#)
- > [F.A.Q.'s](#)

Tokelau Magic

- > [Benefiting the island](#)
- > [Whowhatwhere?](#)
- > [Tokelau snapshots](#)



1A(4)

Universal Case File Number 288A-SF-133411Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document _____

Date Received 1-16-2003 b7CFrom [Redacted]

(Name of Contributor)

(Address of Contributor)

(City and State)

By SA [Redacted] b7CTo Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title:

UNSUB(S);
GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment
01/02/2003Reference: FD-302 1/16/03

(Communication Enclosing Material)

SERIAL 8Description: ☒ Original notes re interview of288A-SF-133411-1A(4)

11:30a

1-14-03

[redacted]

been with Google for

[redacted]

months.)

logs unclear

Work with

[redacted]

on loss estimate,

[redacted]

for many years

b7C

1A(5)

Universal Case File Number 288A-SF-133411Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document _____

Date Received 1-16-2003

From _____

(Name of Contributor)

(Address of Contributor)

(City and State)

By SA b7CTo Be Returned ☐ Yes ☐ NoReceipt Given ☐ Yes ☐ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes ☐ No

Federal Taxpayer Information (FTI)

☐ Yes ☐ NoTitle: UNSUBS,
GOOGLE.COM - VICTIMReference: FD-302 DATED 1/13/03
(Communication Enclosing Material)Serial 9Description: ☐ Original notes re interview ofWHOIS ON b7C288A-SF-133411-1A(5)

[home](#) | [register a new domain](#) | [my DotTK](#) | [about DotTK](#) | [support](#) | [policies](#) | **WHOIS**

WHOIS

WHOIS

Selected domain name:

This is a PAIDDOMAIN.TK domain name. On this domain name the PAIDDOMAIN.TK terms and conditions apply.

The registrant of this domain name is:

Company N/A

Name

Address

Postal code/zipcode

City

State

Country

Phone number

Fax number

Email address

Name servers

b7C

REGISTER A DOMAIN

Find your domain name now!

.tk

OK >>

> Want to know why it's free?

DOT TK SERVICES

Dot TK Domain names

- > [How does it work?](#)
- > [Increasing your traffic](#)
- > [Become a Dot TK Affiliate](#)
- > [Fortune 500 Trademark Trade](#)
- > [F.A.Q.'s](#)

Tokelau Magic

- > [Benefiting the island](#)
- > [Whowhatwhere?](#)
- > [Tokelau snapshots](#)

WHOIS search on another domain name

WWW. .TK

CONTINUE >>

14(6)

Universal Case File Number 288A-SF-133411Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document _____

Date Received 1-16-2003

From _____ b7C

(Name of Contributor) b7D

(Address of Contributor)

(City and State)

By SA _____ b7CTo Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

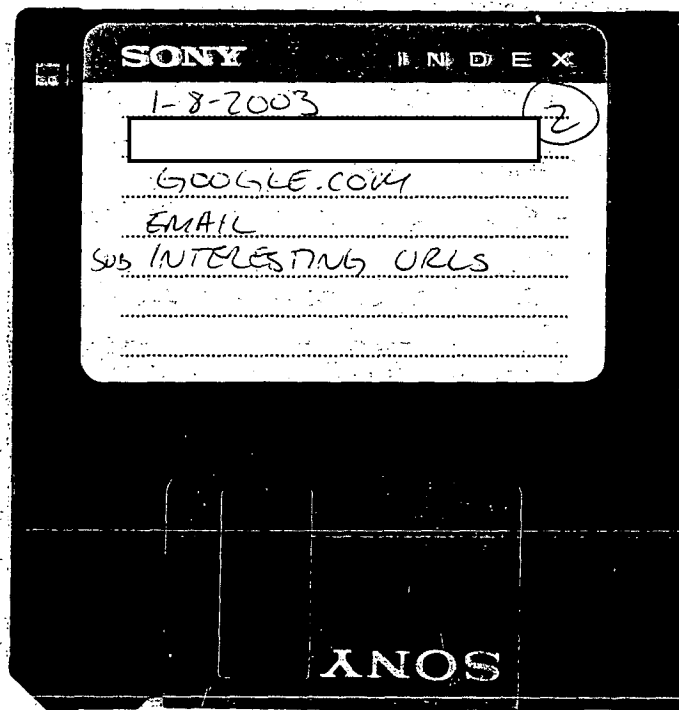
☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ NoTitle: UNSUB(S);
GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment
01/02/2003Reference: FD-302 1/16/03

(Communication Enclosing Material)

SERIAL 10Description: ☐ Original notes re interview ofEMAIL ON 1/8/03288A-SF-133411-14(6)



b7C

b7D

(147)

Universal Case File Number 288A-SF-133411Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document _____

Date Received 1-16-2003

From _____

(Name of Contributor)

(Address of Contributor)

(City and State)

By SA _____

b7C

To Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ NoTitle: UNSUB(S);
GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment
01/02/2003

Reference: _____

(Communication Enclosing Material)

SERIAL 11Description: ☐ Original notes re interview ofEMAIL 1/16/03288A-SF-133411-1A(7)

[HOME](#) | [HELP CENTER](#) | [ACCOUNT CENTER](#) | [ABOUT US](#)[Manage E-mail](#)

View Message

[Manage User ID](#)[Web Mail](#)[Check Mail](#)[New Message](#)[Address Book](#)[Distribution Lists](#)

From:

To: nccs-sf@fbi.gov

b7C

cc:

Date: Thu, January 16, 2003, 12:02:00

Subject: Attention- Agent [redacted] FWS [redacted] incident 01/06/03

b7C

[VIEW HEADER](#) [VIEW BODY](#)[SAVE SENDER](#)[LOG OFF](#)

[redacted]
Below are the incident notes I took for [redacted] bot found on the WIN2k machine administered by [redacted] Waubay National Wildlife Refuge.
I'm making a copy of the Ghosted image to send you right now. Let me know if you need anything else.

b7C

NCC Security Response Team

b2

NOTES:

1/6/03 9am

Called FBI agent [redacted] (Chicago) back regarding voice mail (8am) he left [redacted]

b7C

Notes from FBI conversation:

FBI Case#288a-sf-13341 out of San Fran

Victim IP [redacted]

Exploit- Open shares bot affecting WIN2k machines without admin passwords

IP first joined IRC channel on Jan3rd, 2003, 8:14:29pm GMT (1:14:29 MST), look in logs for IP aquired around that time

Check for listening on ports [redacted] and talking on [redacted]

Possibly being used as an attack platform in [redacted] network.

b7C

I sent note to [redacted] and [redacted] regarding event as FYI.

b2

Called [redacted] and left voice mail regarding event.

Went through [redacted] logs and found IP assigned to user [redacted] during that time.

Copies of relevent log events:

Jan-03-2003 13:13:29 Accounting start record for user [redacted]

start_time=1041624777, timezone=MST, service=ppp

b2

Jan-03-2003 13:47:40 Accounting stop record for user [redacted]

start_time=1041624777, timezone=MST, service=ppp, protocol=ip, addr=[redacted]

b7C

Filled out Incident Response Form and sent to [redacted] and CC:ed [redacted]

[redacted] for her to make initial contact with [redacted] to brief him on the incident.

b7C

Called [redacted] FBI, to inform him we found the victim and recieved directions from him on what to look for, ie, [redacted]

Called [redacted] and informed him that his machine has been hacked and gave him directions to back-up his sensitive data and send machine (just the box) to me at the NCC in Denver. I requested he do nothing to any other files except back up his important ones and that we need the machine for further forensic analysis and will have it for an estimated 4 weeks.

1/8/03

7am- Sent note to [redacted] informing him we should be getting the box this week.

b7C

10am Recieved the box:

Gateway E Series, WIN2k-SP3

Intel P4, 2.0 GHz, 524 Megs RAM

Computer name [redacted]

no modem (must be external, I called and confirmed attached to an external modem)

no admin password

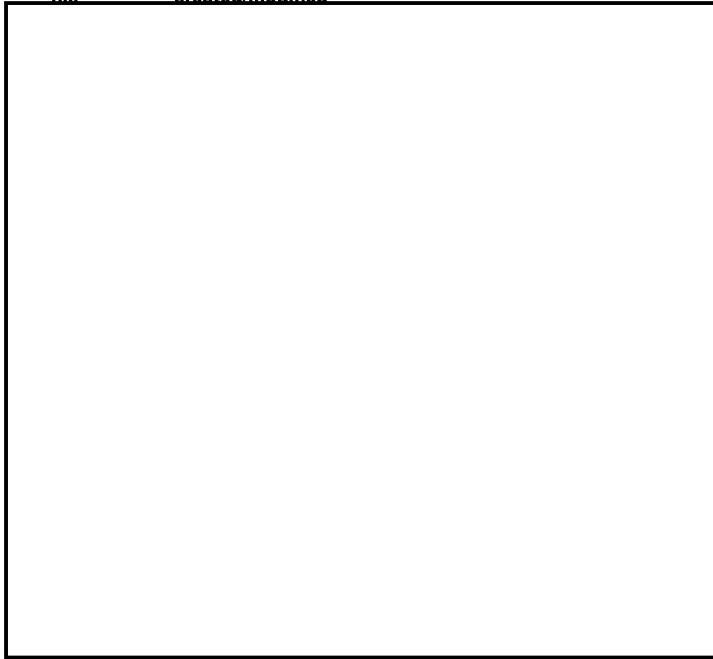
NO mirc.ini file (been removed by [redacted] ???)

b7C

Malware files -

C:\WINNT\system32\dhcp\

file created/modified



b2

Malware services running:

FireDaemon Service: ir Automatic

Serv-U FTP Server Automatic

Website explaining the attack in detail -http: [redacted] EduHacking.html

1/9 - Called [redacted] back at FBI and he said someone from San Fran office will be calling me about the box.

b7C

1/10 - Ghosted image to network. 1.9 gigs.

1/13- Burned image to 3 CDs and removed image from network server. I had [redacted] e-image machine with WIN2000 Pro and give it an admin password. Will send machine back to [redacted] when re-image is complete.

1/16- Sent box back to [redacted] in South Dakota

b7C

[\[X\] FORWARD MAIL](#) [\[X\] REPLY](#) [\[X\] REPLY TO ALL](#) [\[X\] DELETE](#) [\[X\] NEXT MESSAGE](#) [\[X\] RETURN](#) [\[X\] HELP](#)

[LEGAL](#) | [PRIVACY](#) | [SERVICE TERMS](#) | [CONTACT US](#)

Copyright © 2002, AT&T All Rights Reserved.

Received: from [redacted] ov (<unknown.domain>[redacted])
by prserv.net (in4) with ESMTP
id [redacted] Thu, 16 Jan 2003 19:03:34 +0000

To: [redacted]
Cc: [redacted]
Subject: Attention- Agen [redacted] (FWS [redacted] incident 01/06/03)
MIME-Version: 1.0

b7C

X-Mailer: Lotus Notes Release 5.0.10 March 22, 2002

b2

Message-ID: [redacted] gov>

From: [redacted]
Date: Thu, 16 Jan 2003 12:02:58 -0700

[redacted] Serialize by Router on [redacted] at
01/16/2003 12:07:03 PM,

Serialize complete at 01/16/2003 12:07:03 PM

Content-Type: multipart/alternative; boundary="=_alternative [redacted]

1-16-03

EMAIL

b7C

SONY

1A(8)

Universal Case File Number

288A-SF-133411

Field Office Acquiring Evidence

HAYWARD

Serial # of Originating Document

Date Received

1-16-2003

From

(Name of Contributor)

(Address of Contributor)

(City and State)

By

SA

b7C

To Be Returned

☐ Yes☐ No

Receipt Given

☐ Yes☐ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes☐ No

Federal Taxpayer Information (FTI)

☐ Yes☐ No

Title:

Reference:

FD-302 DATED 1-15-2003

(Communication Enclosing Material)

Serial 12

Description:

☐

Original notes re interview of

b7C

WEB PAGES ON DISK+PAPER

288A-SF-133411-12(8)

[redacted]:Contact
You can contact me on [redacted] and/or [redacted] via [redacted] channel

You can also contact me at Contact Me

I am also contactable via telephone, but it is NOT recommended unless it's very urgent, but I can be contacted at [redacted] some phone restrictions may apply, you are responsible for the long-distance telephone bill, not me.

b7C

b2

For sales inquiries contact Sales Department

For support please either visit [redacted] or email Support Department

b7C

Contact[1]

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">

<html>

<head>

<title>Contact us</title>

<meta http-equiv="Content-Type" content="text/html; charset=

</head>

<body bgcolor="#000000" text="#00FF00" link=

alink=

<div align="center">

<p>:Contact

You can contact me on via channel

You can also contact me at Contact
Me

I am also contactable via telephone, but it is NOT recommended unless its very
urgent, but i can be contacted at some phone restrictions may
apply, you are responsible for the long-distance telephone bill, not me.</p>

b7C

b2

<p>For sales inquiries contact Sales
Department

For support please either visit on or email Support

Department</p>

<p> </p>

</div>

</body>

</html>

[redacted] About

[redacted] is owned and maintained by [redacted] and his friends. He can be reached on [redacted]

I can be reached by phone at [redacted]

There's more of a chance you will get helped in either the chatroom(s) or email me at the contact link on the menubar of this site. Thanks.

b7C

[redacted] is here to give you the best prices for the best products we can give! NOTE: We don't get much profit out of this, we charge what it COSTS to keep it running. no more, and there's many sales, reductions available, let's say you refer some people, you will get a discount, or have money refunded back through our merchant system.

b2

[redacted] is here to give you quality services, we do not supply you with "public" Vhost's, or anything like that. You can get "private" vhosts for your self like: yourname [redacted] but not stuff like i.am.a.leet.mof [redacted] we ONLY accept 1 subdomain on the reverse DNS, sorry!

As far as webhosting goes, we only limit you on space, we do not limit your email accounts, parked domains, subdomains or anything! and cPanel is a professional package, which allows easy usage of your webhosting package! you will enjoy it immensely! one click and you can have ecommerce, one click and you can have phpnuke, and much, much more!

b7C



b7C

1A(9)

Universal Case File Number 288A-SF-133411Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document _____

Date Received 1-16-2003

From _____

(Name of Contributor)

(Address of Contributor)

(City and State)

By SA

b7C

To Be Returned ☐ Yes ☐ NoReceipt Given ☐ Yes ☐ NoGrand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure☐ Yes ☐ No

Federal Taxpayer Information (FTI)

☐ Yes ☐ NoTitle: UNSUBS;
GOOGLE.COM - VICTIMReference: INSERT DATED 1-14-03

(Communication Enclosing Material)

SERIAL 13Description: ☐ Original notes re interview ofWHOIS ON

b7C

288A-SF-133411-1A(9)



The .tv Corporation
a VeriSign® company
www.tv

[VIEW OUR SITE IN...](#)[ENGLISH](#) [DEUTSCH](#) [ESPAÑOL](#) [FRANÇAIS](#) [日本語](#) [한국어](#) [繁體中文](#)[HOME](#)[FIND A
DOMAIN](#)[PREMIUM
NAME SHOWCASE](#)[PRODUCTS
+ SERVICES](#)[RENEWAL
CENTER](#)[HELP](#)[SHOPPING CART](#)[MY ACCOUNT](#)[Why .tv?](#) | [Tell a Friend](#) | [Customer Testimonials](#) | [Featured .tv Sites](#) |SEARCH FOR A DOMAIN NAME: www. .tv

WHOIS SEARCH RESULTS

Domain Name:

Record expires on:

Feb 6 2011

Record created on:

Feb 6 2001

Domain Name Servers:

Registrar Name:

Network Solutions

Registrar Whois
Information:

whois.networksolutions.com

The data in The .tv Corp. whois database is provided by The .tv Corp. assist persons in obtaining information about or related to a domain name registration record. .tv does not guarantee its accuracy. By submitting a whois query, you agree that you will use this data only for lawful purposes and that, under no circumstances, will you use this data to allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail (spam). The .tv Corp. reserves the right to modify this policy at any time.

[Transfers](#) | [Whois](#) | [Policies](#) | [Press Room](#) | [Advertise With Us](#) | [Partner Programs](#) | [Multi-Lingual Domain Names](#)© 2002 The .tv Corporation. All Rights Reserved. [Privacy Policy](#)

a VeriSign® company
Network Solutions

HELP WI

[HOME](#) [DOMAIN NAMES](#) [WEB SITES](#) [E-MAIL](#) [BUSINESS BUILDERS](#) [RENEW SERVICES](#) [ACC](#)

► WHOIS Search Results

WHOIS Record for

[Back-order this name](#)[Make an unsolicited offer](#)

Registrant:

b7C

Domain Name:

Administrative Contact:

Technical Contact:

VeriSign, Inc. (HOST-ORG)
VeriSign, Inc.
21355 Ridgetop Circle
Dulles, VA 20166
US
1-888-642-9675

namehost@WORLDNIC.NET

Transfe
domain
for o
\$1
a ye
includes 1 year

Record expires on 04-Feb-2011.

Record created on 06-Feb-2001.

Database last updated on 14-Jan-2003 16:17:01 EST.

Domain servers in listed order:

[SEARCH AGAIN](#)[Search the Web with Dogpile](#)[Yellow Pages-Find a business FAST](#)

NOTICE AND TERMS OF USE: You are not authorized to access or query our WHOIS database through the use of high-volume, automated, electronic processes. The Data in Network Solutions' WHOIS database is provided by Network Solutions for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. Network Solutions does not guarantee its accuracy. By submitting a WHOIS query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to Network Solutions (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of Network Solutions. You agree not to use high-volume, automated, electronic processes to access or query the WHOIS database. Network Solutions reserves the right to terminate your access to the WHOIS database in its sole discretion, including without limitation, for excessive querying of the WHOIS database or for failure to otherwise abide by this policy. Network Solutions reserves the right to modify these terms at any time.

b7C

[Back to top](#) | [About Us](#) | [Partnerships](#) | [Contact us](#) | [Site Map](#)

[Review our Privacy Policy](#), [Service Agreement](#), [Legal Notice](#) and [Disclaimer](#) ©
Copyright 2003 Network Solutions, Inc. All rights reserved.



b7C

1A-C(10)

Universal Case File Number 288A-SF-133411Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document _____

Date Received 1-6-2003From
(Name of Contributor)(Address of Contributor) b7CCHICAGO, IL
(City and State)By SA To Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ NoGrand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ NoTitle: UNSUB(S);
GOOGLE - VICTIM ~~INTERVIEW~~
SUNNYVALE, CA
NIPC - IMPAIRMENT
1/2/2003Reference: FD-302 DATED 1-6-2003
(Communication Enclosing Material)SERIAL 24Description: ☐ Original notes re interview ofFLOPPY DISK CONTAINING EMAIL AND
ATTACHMENTS (1-6-2003, 13:30:00)288A-SF-133411-1A-C(10)

SONY

I N D E X

7-6-2003

b7C

ANCH

1A(11)

Universal Case File Number 288A-SF-133411Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document _____

Date Received 1-8-2003From [Redacted]

(Name of Contributor)

(Address of Contributor)

b7C

(City and State)

By SA [Redacted]To Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ NoTitle: UNSUB(S);
GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - IMPAIRMENT
01/02/2003Reference: FD-302 DATED 1-8-2003

(Communication Enclosing Material)

SERIAL 25Description: ☒ Original notes re interview of

b7C

288A-SF-133411-1A(11)

2881A -SF -133411

1-7-03

b7C

(c)

(u)

[REDACTED] HAVE ADDRESS

2:17p

RANGE

b7D

- ~~NO~~ GOOGLE RESEARCHED, ONE IP CONNECTED 3
ATTACK

b7C

TIMES DURING DAY, LINKS BACK TO [REDACTED]

AM - SPIKE OF INCOMING TRAFFIC - CORRESPONDS TO TIME
OF COMMANDS ON IRC CHANNEL

PM - SAME, [REDACTED]

ATTACK IN AM INDICATES [REDACTED]

[REDACTED]
STARTING TO [REDACTED]

[REDACTED]
SHOULD HAVE [REDACTED]

2:29p

1A(12)

Universal Case File Number 288A-SF-133411

Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document

Date Received 1/21/03

From

(City and State)

~~—~~b7C

By

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

**Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure**

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title:

L.k.a.

GOOGLE – VICTIM
SUNNYVALE, CA
NIPC – Impairment

b7C

b3

Reference:

(Communication Enclosing Material)

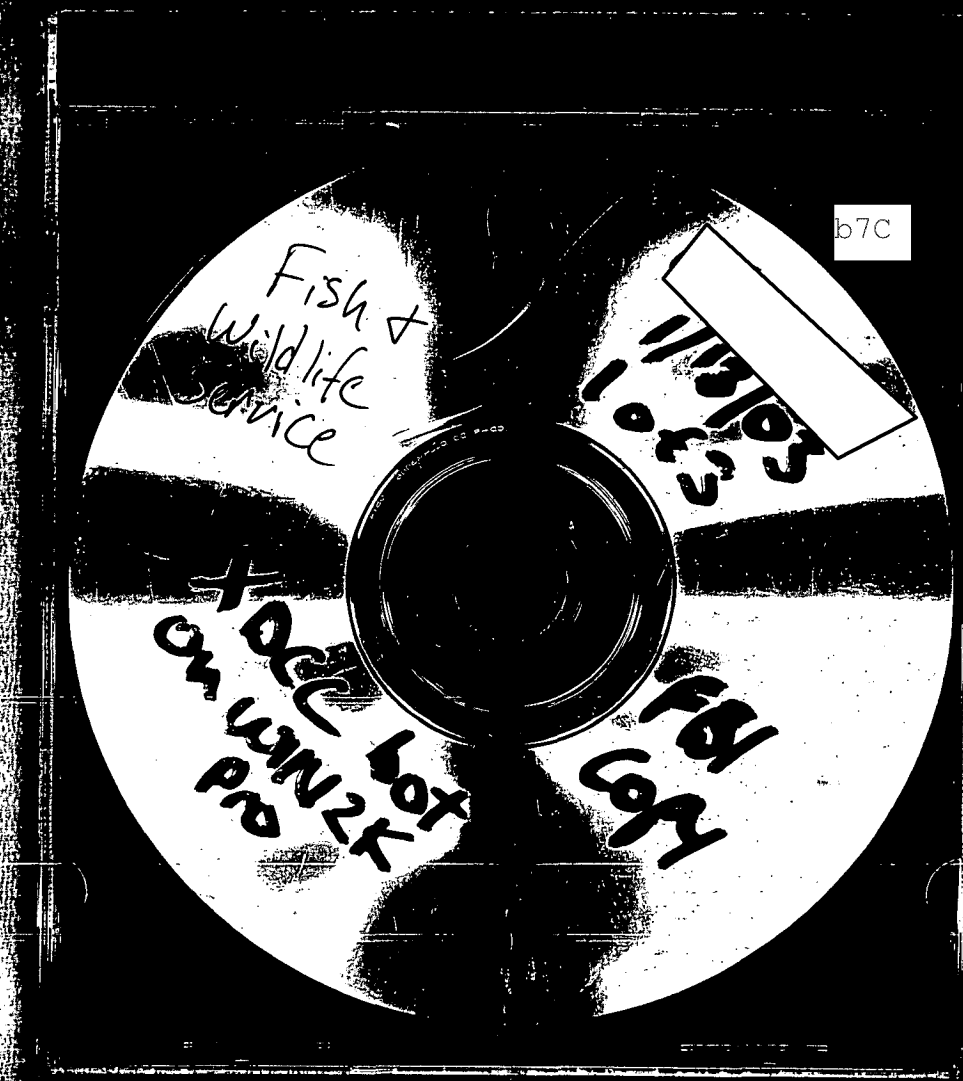
b2

Description: ☐ Original notes re interview of

b7C

CN'S OF	MACHINE FROM FWS
---------	------------------

288A-GF-133411-1A(12)



**WOULD YOU RATHER HAVE
WWW.THISWASTHEONLYNAMELEFT.COM...**

[Domain
Info](#)

[Domain
Search](#)

[Register.com](#)

[Reverse IP
Lookup](#)

[Trace
Route](#)

[Hot
Topics](#)

[Home Contacts](#)

Domain Info

eAmnesia.com

The Domain Name Search Engine™

Here you can get information about the selected domain. The query result includes owner name, contacts and other useful information. The query works with **com/net/org (ICANN and CORE)** as well as **gov, mil, edu** and most of the two letter country DNS zones (like **co.uk** or **ru**).

Tips:

- Type an IP address instead of the domain name for the reverse query or go to the "[Reverse IP Lookup](#)" for more information about a host with known IP address.
- If you are not certain about the name of the site, use [DNS search screen](#) to find it. It includes search by separate parts, fuzzy search, similar to a spellchecker and other powerful features. After you find the name, follow the (i) link to see information from this page.

Domain Name:	<input type="text"/>	<input type="button" value="Get Domain Info"/>	<input type="text" value="adomain.com"/>
--------------	----------------------	--	--

IP Information

b7C

**WOULD YOU RATHER HAVE
WWW.THISWASTHEONLYNAMELEFT.COM...**

b7C

**WOULD YOU RATHER HAVE
WWW.THISWASTHEONLYNAMELEFT.COM...**

[Domain
Info](#)

[Domain
Search](#)

[Register.com](#)

[Reverse IP
Lookup](#)

[Trace
Route](#)

[Hot
Topics](#)

[Home Contacts](#)

Reverse IP Lookup

eAmnesia.com

The Domain Name Search Engine™

This is the powerful tool to find information about an Internet host by its IP address. The result includes information about owner of the IP address, its DNS name(s) and so on. The lookup works against any IP address on the Internet. This utility is much more powerful, then reverse IP lookup.

Just in case, IP address looks like four numbers, separated by dots (For example 192.168.12.34) If you have one long number (like 132468197), type or copy/paste it in the field for the whole address and press "Convert" button to translate it to canonical form.

Tips:

- Use the "whole address" field if you want to copy/paste the IP address from the clipboard.
 - While entering IP address into separate fields, type dot on the keyboard to jump to the next fields.
- Unfortunately it does not work on every version of the browser.

IP Address:	<input type="text"/>	Lookup Name	<input type="text"/>
Or type it here:	<input type="text"/>	Convert	<input type="text"/>

Result of the Reverse Lookup

IP address	Result
<input type="text"/>	

b7C

b2

WHOIS Query Result for

OrgName:

OrgID:

NetRange:

CIDR:

NetName:

NetHandle:

Parent:

NetType:

NameServer:

NameServer:

Comment:

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

RegDate:

2002-05-31

Updated:

2002-05-31

TechHandle: ZMA1-ARIN

TechName:

TechPhone:
TechEmail:

b7C

ARIN Whois database, last updated 2003-01-22 20:00
Enter ? for additional hints on searching ARIN's Whois database.

1A(14)

Universal Case File Number 288A-SF-133411Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document _____

Date Received 1/23/03

From _____

(Name of Contributor)

(Address of Contributor)

(City and State)

By SATo Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

(UNSUB(S);
Title: GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment
01/02/2003

Reference: FD-302 1/23/03

(Communication Enclosing Material)

Serial 30Description: ☐ Original notes re interview ofIP SCAN288A-SF-133411-1A(14)

b7C

b7C

**WOULD YOU RATHER HAVE
WWW.THISWASTHEONLYNAMELEFT.COM...**

Domain Info

Domain Search

Register.com

Reverse IP Lookup

Trace Route

Hot Topics

Home Contacts

Domain Info

eAmnesia.com

The Domain Name Search Enginetm

Here you can get information about the selected domain. The query result includes owner name, contacts and other useful information. The query works with **com/net/org (ICANN and CORE)** as well as **gov, mil, edu** and **most of the two letter country DNS zones (like co.uk or ru)**.

Tips:

- Type an IP address instead of the domain name for the reverse query or go to the "Reverse IP Lookup" for more information about a host with known IP address.
- If you are not certain about the name of the site, use DNS search screen to find it. It includes search by separate parts, fuzzy search, similar to a spellchecker and other powerful features. After you find the name, follow the (i) link to see information from this page.

Domain Name:	<input type="text"/>	Get Domain Info	<input type="text" value="adomain.com"/>
---------------------	----------------------	---------------------------------	--

IP Information

[redacted] web site]	
[redacted] host not found	Use "The Domain Search" to find it.
[redacted] ftp site]	
[redacted] host not found	Use "The Domain Search" to find it.

b7C

**WOULD YOU RATHER HAVE
WWW.THISWASTHEONLYNAMELEFT.COM...**

**WOULD YOU RATHER HAVE
WWW.THISWASTHEONLYNAMELEFT.COM...**

[Domain
Info](#)

[Domain
Search](#)

[Register.com](#)

[Reverse IP
Lookup](#)

[Trace
Route](#)

[Hot
Topics](#)

[Home Contacts](#)

Reverse IP Lookup

eAmnesia.com

The Domain Name Search Engine^{III}

This is the powerful tool to find information about an Internet host by its IP address. The result includes information about owner of the IP address, its DNS name(s) and so on. The lookup works against any IP address on the Internet. This utility is much more powerful, then reverse IP lookup.

Just in case, IP address looks like four numbers, separated by dots (For example 192.168.12.34) If you have one long number (like 132468197), type or copy/paste it in the field for the whole address and press "Convert" button to translate it to canonical form.

Tips:

- Use the "whole address" field if you want to copy/paste the IP address from the clipboard.
- While entering IP address into separate fields, type dot on the keyboard to jump to the next fields. Unfortunately it does not work on every version of the browser.

IP Address:	<input type="text"/>	Lookup Name	<input type="text"/>
Or type it here:	<input type="text"/>	Convert	<input type="text"/>

Result of the Reverse Lookup

IP address	Result
	net [more info for this domain name]

WHOIS Query Result for

OrgName:
OrgID:

b7C

NetRange:

CIDR:

NetName:

NetHandle:

Parent:

NetType:

Direct Allocation

NameServer

NameServer

Comment:

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

RegDate:

1999-09-14

Updated:

2001-01-04

TechHandle:

TechName: Network Administrator, CyberGate

b2

b7C

TechPhone:

TechEmail:

ARIN Whois database, last updated 2003-01-22 20:00

Enter ? for additional hints on searching ARIN's Whois database.

ValueWeb
An Affinity Company

1.800.WE.HOST.U
1.800.934.6788

[HOME](#) [CONTACT](#)

[HOSTING PLANS](#)

[DEDICATED HOSTING](#)

[RESELLERS](#)

[SUPPORT](#)

[ABOUT US](#)

[SIGN UP NOW](#)

Search for a NEW
Domain Name Here!

.com

SEARCH



Contact Us

Your questions and comments are important to us.

Shared Hosting

Call Me Back

Never wait on hold again! Have a representative call you. (Available in over 190 countries.)

- Sales 24 hours a day, 7 days a week
- Technical Support 7 days a week, 24 hours a day.
- Customer Service Mon - Fri, 9am - 10pm ET

Let's Chat

Chat online with a representative.

- Sales Mon - Fri, 8am - 9pm ET
- Technical Support 7 days a week, 9am - 10pm ET
- Customer Service Mon - Fri, 9am - 5:30pm ET

Search our Solution Database **GO**

A database of customers' most Frequently Asked Questions (FAQs), arranged by popularity and searchable by keyword.

Email Your Question

If you don't find your answer in the Solution Database, email your question and we'll provide a detailed response within 24 hours.

Contact Us By Phone:

Sales

Sales Numbers:
1-800-WE-HOST-U
800.934.6788
954.334.3871

International Toll Free Sales Numbers:

UK	00-800-7888-7888
Germany	0 0-800-7888-7888
Ireland	0 0-800-7888-7888
New Zealand	0 0-800-7888-7888
Australia	0 011-800-7888-7888
Japan	0 061-800-7888-7888 IDC 001-800-7888-7888 KDD 0041-800-7888-7888 ITJ

Tech Support

Technical Support Hours:
24 hours / day - 7 days / week

Technical Support Numbers:
800.522.1093
954.334.3449

Customer Service

Customer Service Hours:
Monday - Friday: 9am - 10pm ET
Saturday - Sunday: Closed

Customer Service Numbers:
800.522.1093
954.334.3449

Dedicated Hosting

Let's Chat

Chat online with a representative.
• Sales 24 hours a day, 7 days a week

Access Support

Email us support-related inquiries, search solution database, manage your account

Contact Us By Phone:

Sales

Sales Hours:

Customer Service

Customer Service Hours:

24 hours / day - 7 days / week

Sales Numbers:

888.846.5522
954.334.8333 (US & International)
Fax 954.334.8005

Monday - Friday: 9am - 5pm ET
Saturday - Sunday: Closed

Customer Service Numbers:

888.846.5522
954.334.8333 (US & International)

Tech Support

Technical Support Hours:
24 hours / day - 7 days / week

Technical Support Numbers:

888.846.5522
954.334.8333 (US & International)

Corporate Headquarters

Corporate Headquarters

Address:
3250 W. Commercial Blvd.
Ft. Lauderdale, FL 33309

Phone Number
954.334.8000

FAX Number:
954.334.8001

TERMS AND POLICIES | COPYRIGHT ©2002 AFFINITY INTERNET INC.

CALL NOW! 1.800.W
11

1A(15)

Universal Case File Number 288A-SF-133411Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document _____

Date Received 1/23/03

From _____

(Name of Contributor)

(Address of Contributor)

(City and State)

By SA b7CTo Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ NoTitle: UNSUB(S);
GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment
01/02/2003Reference: FD-302 1/23/03

(Communication Enclosing Material)

Serial 31Description: ☐ Original notes re interview of IP SCAN b7C288A-SF-133411-1A(15)

**WOULD YOU RATHER HAVE
WWW.THISWASTHEONLYNAMELEFT.COM...**

[Domain
Info](#)

[Domain
Search](#)

[Register.com](#)

[Reverse IP
Lookup](#)

[Trace
Route](#)

[Hot
Topics](#)

[Home](#) [Contacts](#)

Domain Info

eAmnesia.com

The Domain Name Search Engine™

Here you can get information about the selected domain. The query result includes owner name, contacts and other useful information. The query works with **com/net/org (ICANN and CORE)** as well as **gov, mil, edu** and **most of the two letter country DNS zones (like co.uk or ru)**.

Tips:

- Type an IP address instead of the domain name for the reverse query or go to the "[Reverse IP Lookup](#)" for more information about a host with known IP address.
- If you are not certain about the name of the site, use [DNS search screen](#) to find it. It includes search by separate parts, fuzzy search, similar to a spellchecker and other powerful features. After you find the name, follow the (i) link to see information from this page.

Domain Name:	<input type="text"/>	<input type="button" value="Get Domain Info"/>	<input type="text" value="adomain.com"/>
--------------	----------------------	--	--

IP Information

<input type="text"/>	<input type="text"/>
	<input type="text"/>
	<input type="text"/>
host not found Use "The Domain Search" to find it.	
<input type="text"/>	<input type="text"/>

b7C

**WOULD YOU RATHER HAVE
WWW.THISWASTHEONLYNAMELEFT.COM...**

**WOULD YOU RATHER HAVE
WWW.THISWASTHEONLYNAMELEFT.COM...**

[Domain
Info](#)

[Domain
Search](#)

[Register.com](#)

[Reverse IP
Lookup](#)

[Trace
Route](#)

[Hot
Topics](#)

[Home](#) [Contacts](#)

Reverse IP Lookup

eAmnesia.com

The Domain Name Search Enginetm

This is the powerful tool to find information about an Internet host by its IP address. The result includes information about owner of the IP address, its DNS name(s) and so on. The lookup works against any IP address on the Internet. This utility is much more powerful, then reverse IP lookup.

Just in case, IP address looks like four numbers, separated by dots (For example 192.168.12.34) If you have one long number (like 132468197), type or copy/paste it in the field for the whole address and press "Convert" button to translate it to canonical form.

Tips:

- Use the "whole address" field if you want to copy/paste the IP address from the clipboard.
- While entering IP address into separate fields, type dot on the keyboard to jump to the next fields. Unfortunately it does not work on every version of the browser.

IP Address:	<input type="text"/>	Lookup Name	<input type="text"/>
Or type it here:	<input type="text"/>	Convert	<input type="text"/>

Result of the Reverse Lookup

IP address	Result
<input type="text"/>	

b7C

WHOIS Query Result for

b2

OrgName: One Call Communications
OrgID: OCCI

NetRange:
CIDR:
NetName:
NetHandle:
Parent:
NetType: Direct Allocation
NameServer:
NameServer:
Comment: ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
RegDate: 2002-01-30
Updated: 2002-10-16

NOCHandle: TECHN2-ARIN
NOCName: Technical Contact

NOCPhone: +1-888-223-8633

NOCEmail: noc@onecall.net

NOCHandle: DNSTE-ARIN

NOCName: DNS Technical

NOCPhone: +1-888-223-8633

NOCEmail: dnstech@onecall.net

b7C

TechHandle: TW66-ARIN

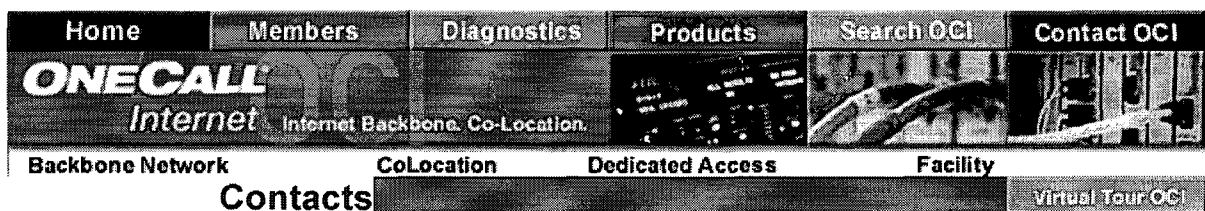
TechName:

TechPhone

TechEmail

ARIN Whois database, last updated 2003-01-22 20:00.

Enter ? for additional hints on searching ARIN's Whois database.



General Comments

webmaster@onecall.net

Technical Sales

888-223-8633 9-5 EST Mon-Fri
techsale@onecall.net

Security/UCE Complaints/Questions
Acceptable Use Policy (AUP)
[Complaint Guidelines](#) (please read)

abuse@onecall.net

NAP/MAE Peering Ops

peering@onecall.net

NOC Technical Support

888-223-8633 24x7x365
noc@onecall.net

Billing Inquiries

888-223-8633 9-5 EST Mon-Fri

[\[Home\]](#) [\[Member Services\]](#) [\[Diagnostics\]](#) [\[Products\]](#) [\[Search\]](#) [\[Contact OCI\]](#)
© One Call Internet. webmaster@onecall.net

1A(16)

Universal Case File Number

288A-SF-133411

Field Office Acquiring Evidence

Chicago

Serial # of Originating Document

Date Received

1/8/03

From

SOURCE

(Name of Contributor)

(Address of Contributor)

(City and State)

b7C

By

SA

To Be Returned ☐ Yes☒ NoReceipt Given ☐☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes☒ No

Federal Taxpayer Information (FTI)

☐ Yes☒ No

Title:

UNSUB(S)

GOOGLE-VICTIM

SUNNYVALE, CA

NRC IMPAIRMENT

Reference:

EC 1/8/03

(Communication Enclosing Material)

Serial 20

Description:

☐

Original notes re interview of

SOURCE EMAIL

288A-SF-133411-1A(16)

288A-SF-113411
1/8/3 MDA

J51364108262149118 8.0

SOURCE EMAIL
ON

b7C

1A(17)

Universal Case File Number

288A-SF-133411

Field Office Acquiring Evidence

HAYWARD

Serial # of Originating Document

Date Received

1-31-03

From

§

(Name of Contributor)

(Address of Contributor)

b7C

(City and State)

By

SA

To Be Returned

☐

Yes

☒

No

Receipt Given

☐

Yes

☒

No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐

Yes

☒

No

Federal Taxpayer Information (FTI)

☐

Yes

☒

No

Title:

GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment

b7C

b3

Reference:

FD-302 DATED 1-31-03,

(Communication Enclosing Material)

Serial 28

Description:

☐

Original notes re interview of

b7C

EMAIL FROM

WITH

BOT ATTACHMENTS

288A-SF-133411-1A(17)

SONY

1-31 EMAIL FROM

b7C

ANOS

1A (18)

Field File No. 288A-SF-133411

Serial # of Originating Document _____

OO and File No. _____

Date Received 1/10/03From SOURCE
(Name of Contributor)

(Address of Contributor)

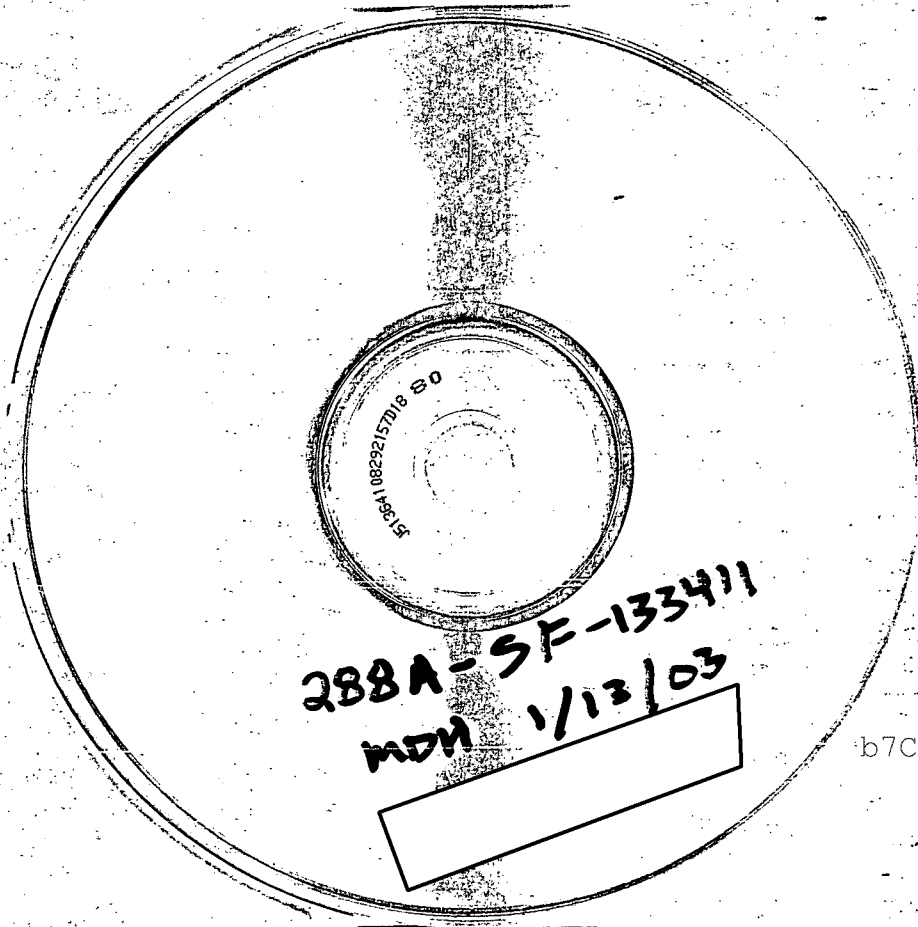
By
(Name of Special Agent)

b7C

To Be Returned ☐ Yes ☒ No Receipt Given ☐ Yes ☒ NoGrand Jury Material - Disseminate Only Pursuant to Rule 6(e), Federal Rules
of Criminal Procedure ☐ Yes ☒ NoTitle: UNSUB(S)
GODDIE VICTIM
SUNNYVALE, CA
NIPC ImpairmentReference: _____
(Communication Enclosing Material)Description: ☐ Original notes re interview of1 CD-R containing WRC log

b7C

288A-SF-133411-1A(18)



b7C

1A(19)

Universal Case File Number

288A-SF-133411

Field Office Acquiring Evidence

HAYWARD

Serial # of Originating Document

Date Received

2/13/03

From

(Name of Contributor)

GOOGLE

b7C

(Address of Contributor)

(City and State)

By

SA

To Be Returned

☐ Yes☒ No

Receipt Given

☐ Yes☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes☒ No

Federal Taxpayer Information (FTI)

☐ Yes☒ No

b7C

Title:

GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment

b3

Reference

FD302 2/13/03

(Communication Enclosing Material)

Description:

☐

Original notes re interview of

EMAIL

288A-SF-133411-1A(19)

[att.com home](#) [AT&T Business](#)[HOME](#) | [HELP CENTER](#) | [> ACCOUNT CENTER](#) | [ABOUT US](#)[MANAGE E-MAIL](#)

View Message

[MANAGE USER ID](#)[WEB MAIL](#)[Check Mail](#)[New Message](#)[Address Book](#)[Distribution Lists](#)

From:

[SAVE SENDER](#)

To:

cc:

Date: Thu, February 13, 2003, 11:18:00

Subject: Attn: **CONFIDENTIAL**[VIEW HEADER](#)[VIEW BODY](#)

b7C

[LOG OFF](#)

Attached is the estimate of our damages from the January 2 denial of service attack. As I mentioned we have experienced additional attacks since then and would like to report the details to you as soon as possible. Can you let me know when you might be able to visit?

Regards



ddos_damages.doc

[FORWARD MAIL](#)[REPLY](#)[REPLY TO ALL](#)[DELETE](#)[NEXT MESSAGE](#)[RETURN](#)[HELP](#)[LEGAL](#) | [PRIVACY](#) | [SERVICE TERMS](#) | [CONTACT US](#)

Copyright © 2002, AT&T All Rights Reserved.

To: [REDACTED] FBI

b7C

From: [REDACTED] VP and General Counsel, Google

Per our conversation the other day, the following is our preliminary estimate of the economic loss Google suffered from the distributed denial of service attacks that took place on January 2, 2003:

1. Lost Revenue. The attacks caused us to lose search queries that would otherwise have been performed on our and our partners' sites. We generate revenue from these queries through our various advertising programs. We estimate these losses at approximately \$5,000.
2. Potential Liability to Search Partners: The loss of queries on certain of our partners' sites may subject us to penalties under the service level agreements with those partners. We estimate these losses at approximately \$40,000.
3. Employee and Management Time. Our operations employees, certain engineers and our management team spent a significant amount of time responding to the attacks and managing relations with our customers and others. We estimate these losses at approximately \$4,500.

Please note that these are preliminary estimates that may increase as we continue our investigation. Please do not hesitate to contact me if you have any questions. I can be reached at [REDACTED]

b7C

1A(20)

Universal Case File Number 288A-SF-133411Field Office Acquiring Evidence Chicago

Serial # of Originating Document _____

Date Received 02/20/03From SOURCE

(Name of Contributor)

(Address of Contributor)

(City and State)

By SA

b7C

To Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ NoGrand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

b7C

b3

Title:

Google - Uction
Sunnydale, CA
NIPC - Impairment

Reference:

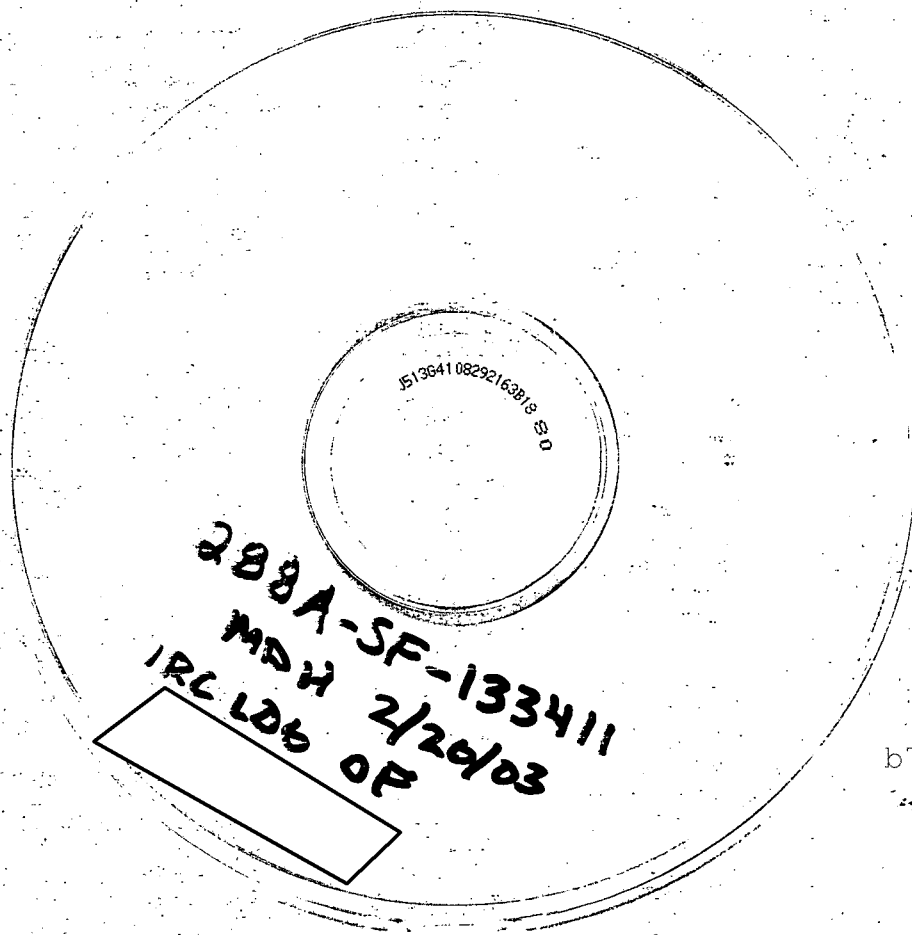
(Communication Enclosing Material)

EC 2/2/03, Serial 46Description: ☐ Original notes re interview ofone (1) CDK with IRE log of channel

b7C

b7D

288A-SF-133411-1A(20)



J51364108292163818 So

288A-SF-133411
MDH 2/26/03
IRC LOG OF

b7C

1A(21)

Universal Case File Number 288A-SF-133411Field Office Acquiring Evidence HAYWARDSerial # of Originating Document 33

Date Received _____ b3 Rule 6(e) _____

From _____
(Name of Contributor)_____
(Address of Contributor)_____
(City and State)By SA _____ b7CTo Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure
☒ Yes ☐ NoFederal Taxpayer Information (FTI)
☐ Yes ☒ No

Title: _____

GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - ImpairmentReference: SERIAL 33
(Communication Enclosing Material)Description: ☐ Original notes re interview ofSUBPOENA RETURN

b3 Rule 6(e) -

288A-SF-133411-1A(21)

1A(22)

Universal Case File Number 288A-SF-133411Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document _____

Date Received 4/16/2003From

(Name of Contributor)

DELAWARE S.P.

(Address of Contributor)

b7C

(City and State)

By SA To Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ NoGrand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title:

GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment

b7C

b3

Reference FD-302 4/16/03

(Communication Enclosing Material)

Description: ☒ Original notes re interview of

b3

PHOTO ON 3.5" FLOPPY OF NOTES FROM PHONE CALL

b7C

FAX OF ITEM SEIZEDNOTES FROM ON APP + APP

Delaware State Police Trp. 4

Financial Crimes Unit,

23652 Shortly Rd., Georgetown, DE 19947

FAXDate: **Wednesday, April 16, 2003**

Number of pages including cover sheet: _____

To:

Special Agent [redacted]

FBI Office - San Francisco

NIPCIP Squad - Hayward RA

Phone: [redacted]

Fax phone: [redacted]

CC:

Case File

From:

Det. [redacted]

Delaware State Police Trp. 4

Financial Crimes Unit

23652 Shortly Rd.

Georgetown, DE 19947

Phone: [redacted]

Pager: [redacted]

E-mail: [redacted]

Fax phone: [redacted]

REMARKS:



Urgent



For your files



Reply ASAP



Please comment

[redacted]
Here are the documents you requested. I gave [redacted] a copy of the search/arrest warrants as well as my report.
I will forward the tape and a CD with Digital images as soon as I can get them packed up.

b7C

b7C

Superior Court Search Warrant
State vs. [redacted]

b7C

b3

Delaware State Police
Search Warrant Seized Property Inventory

Page 4 of 2

b2

Item #	Location Seized	Date	Time	Description of Item
1	Computer Desk	04/15/2003	12:31	Wirespeed Box w/powercord & cable, Mode [redacted]
2	Computer Desk	04/15/2003	12:35	Linksys DSL Router w/ 2 CAT5 cables attached. S/N [redacted]
3	Computer Desk	04/15/2003	12:41	IBM Black Mouse Mode [redacted]
4	Computer Desk	04/15/2003	12:44	(11) Compact Disk-Recordable (CD-R) from top of Dell Computer
5	Computer Desk	04/15/2003	12:54	Misc Cable & Mic, gray USB cable, Sharp PDA cradle w/power cord, Powered USB Hub w/cord, Dell Tower Power Cord
6	Computer Desk	04/15/2003	12:56	Dell Keyboard [redacted]
7	Computer Desk	04/15/2003	12:56	(2) Dell Speakers w/ power supply and connection cables
8	Computer Desk	04/15/2003	12:56	Dell Tower Computer Dimension 4500 Model DHM S/N [redacted] Running Windows XP
9	Computer Desk	04/15/2003	13:04	I-Box (from [redacted] mini tower S/N [redacted] Running Linux [redacted]
10	Computer Desk	04/15/2003	13:05	NEC Monitor S/N [redacted]
11	Computer Desk	04/15/2003	13:04	Monthly Billing Statement from [redacted] w/ Defendant's Address, (1) PNC MAC receipt
12	Computer Desk	04/15/2003	13:14	Silver Optical Mouse Mode [redacted] Silver Zippy Keyboard S/N [redacted] Power Cord to I-Dot Computer, (2) Altec-Lansing Speakers w/ power cord
13	Computer Desk	04/15/2003	13:15	Aiptek VGA Digital Camera w/cradle & USB Cord S/N [redacted]
14	Computer Desk	04/15/2003	13:30	(14) Compact Disk-Recordable (CD-R), (2) Mini Compact Disk-Recordable (CD-R), (1) Plastic Jewel Case)
15	Computer Desk	04/15/2003	13:30	Bundle of Numerous Compact Disk-Recordable (CD-R)
16	Computer Desk	04/15/2003	13:30	(3) Compact Disk for program "Delta Force", 2 Compact Disk for program Battlefield 1942, Manual Battlefield 1942, Lord of the Rings Case w/ 2 Compact Disks, Tiberian Sun Case w/2 Compact Disks, America's Arm Compact Disk, Windows NT Compact Disk, Lexmark X-83 Print Driver CD, 3.5" Diskette Marked "Student Activities"
17	Computer Desk	04/15/2003	13:32	[redacted] Folder with Numerous Compact Disks
18	Computer Desk	04/15/2003	13:39	Financial Papers, Tax Papers, Business License all for [redacted] Fax cover sheet w/email address [redacted] (2) Money Mover debit cards w/defendant's name on it and the Card Holder Agreement statement.
19	Computer Desk	04/15/2003	13:40	Dell Monitor w/power cord and cable, Mode [redacted]
20	Computer Desk	04/15/2003	13:46	Lexmark Printer/Fax/Copier model X83 w/ PNC check # [redacted]
21	Computer Desk	04/15/2003	13:49	Gray CD case with numerous Compact Disks
22	Kitchen Counter	04/15/2003		"Quake III" game CD, (11) Compact Disks
23	Kitchen Counter	04/15/2003		(5) Compact Disk-Recordable, (3) Mini Compact Disk-Recordable
24	Kitchen Counter	04/15/2003		Vivitar Digital Camera w/ gray case (S/N [redacted])
25	Kitchen Counter	04/15/2003		(1) Smart Card reader & USB T-100 Port [redacted]

Investigating Officer [redacted]
DSP Troop 4

Officer Signat [redacted]

b7C

b7D

03 12:04

b2
b7C

DSP TROOP 4

PAGE 02

Superior Court Search Warrant
State vs [REDACTED]

b7C

b3

Delaware State Police
Search Warrant Siezed Property Inventory

Page 2 of 2

Item #	Location Seized	Date	Time	Description of Items
26	Kitchen Counter	04/15/2003		Linksys DSL Router Manual, Dell Computer Account Information, Money Order Receipt, Unauthorized Credit Card Transaction Paperwork, Fedex Envelope & receipt, Various County Bank Papers, PNC Bank papers, Sharp "Personal Digital Assistant (PDA) manual, Windows XP manual, Red Hat Manual, PayPal Fax Cover, Staples Receipt for ethernet adapter.
27	Kitchen Counter	04/15/2003		Battlefield 1942 Box, Sharp PDA program CD, Quake III Arena Team Case and CD, XS Case and Game, Back Digital Camera Case, USB Power Centry Hub w/power cord.
28	Kitchen Table Area	04/15/2003		Quantum Fireball hard drive 3.5"
29	Suspect Bedroom	04/15/2003		Receipts from Staples Office Supply and Register.Com (Top of Dresser)
30	Suspect Bedroom	04/15/2003		Shipping Box from UPS (Top Shelves)
31	Suspect Bedroom	04/15/2003		Sharp Personal Digital Assistant (Left side 2nd drawer of Dresser)
32	Suspect Bedroom	04/15/2003		(1) Compact Disk-Recordable under bed

End of List

b2

Investigating Officer [REDACTED]
DSP Troop 4

b7C

b7D

[Signature]
[REDACTED]

Officer Signature

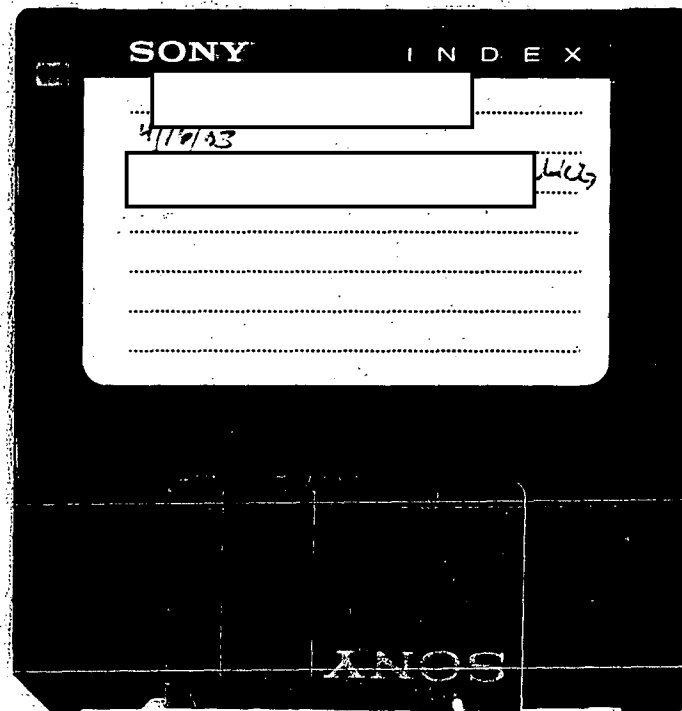
04/16/2003 12:04

DSP TROOP 4

PAGE 03

b7C

b3



1A(23)

Universal Case File Number 288A-SF-133411Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document _____

Date Received 4/22/03From

(Name of Contributor)

DSPD.

(Address of Contributor)

b7C

(City and State)

By SA To Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ NoGrand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ NoTitle:

b7C

b3

GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - ImpairmentReference: FD 302 4/22, SERIAL 18

(Communication Enclosing Material)

Description: ☒ Original notes re interview of

b7C

288A-SF-133411-1A(23)

1105a 4/22/03

POs

b7C

INTERVIEW

[REDACTED] MOM - REFUSED TO PAY \$ TO LET
HIM OUT

UPS DELIVERED A BUNCH OF PKGS

[REDACTED] PD BE POSSIBLY INTERVIEWED,
IN SOME FAMILY CUSTODY

b7C

b3

dy

1A(24)

Universal Case File Number 288A-SF-133411Field Office Acquiring Evidence AA

Serial # of Originating Document _____

Date Received 4-15-03

From _____

(Name of Contributor)

(Address of Contributor)

(City and State)

By _____

b7C

To Be Returned ☐ Yes ☐ NoReceipt Given ☐ ☐ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes ☐ No

Federal Taxpayer Information (FTI)

☐ Yes ☐ No

Title:

Reference: FD 302 4/15/03

(Communication Enclosing Material)

Description: ☒ Original notes re interview of

b7C

b3

288A-SF-133411-1A(24)